Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Policies and Rules Concerning Toll Fraud	)	CC Docket No. 93-292
	)	

Reply Comments of Northern Telecom Inc.

Northern Telecom Inc. ("Northern Telecom") hereby responds to the comments submitted January 14, 1994, on the Commission's Notice of Proposed Rulemaking addressing the issue of policies and rules concerning toll fraud.

Northern Telecom agrees with the statements of commentors, including WilTel, Bell Atlantic, BellSouth, Sprint and Southwestern Bell Telephone, promoting stronger legislation and prosecution of the criminals compromising PBX systems for their own profit. The recent legislation adopted by California (Attachment A) is an excellent example of strengthening the law on telephone fraud and abuse so that stronger deterrents are in place.

Northern Telecom also agrees with MCI and TCA that manufacturers and vendors, along with service providers, have an obligation to inform their customers about the possibility of fraud and abuse. As detailed in its initial comments, Northern Telecom believes it has educated its users, increased security features in its software (Attachment B), recognized the problems customers and distributors face, and provided tools such as system audits to assist in recognizing and controlling unauthorized access. Northern Telecom maintains that it has been constant and consistent in its efforts to increase toll fraud awareness in the following ways: strengthening the security of its software, publishing newsletters, technical documentation, and toll fraud prevention information, holding seminars and training courses, and developing tools to audit its products. All of these proactive steps demonstrate Northern Telecom's commitment to our users and our distributors. Thus, any claims of inaction by manufacturers are inapplicable to Northern Telecom.

Northern Telecom requests that, if a Federal Advisory Committee ("FAC") is created and the Toll Fraud Prevention Committee ("TFPC") is the foundation of the FAC, then the Commission must ensure the fair and broad representation of the telecommunications industry. Northern Telecom urges the Commission to include on the Committee PBX manufacturers, fraud prevention system manufacturers, and PBX distributors, in addition to the exchange carriers that currently comprise the TFPC. Northern Telecom is very interested in toll fraud prevention, and if appointed to the FAC by the Commission, it will commit the resources necessary to participate actively in the work of the Committee as a representative of the PBX manufacturers.

Finally, Northern Telecom supports the comments of the North American Telecommunications Association regarding a manufacturer's limited control of its distributors and products once sold and installed. The permeation of the "gray" market and the difficulty in tracking equipment years after the original sale makes it nearly impossible for a manufacturer to know who currently owns a PBX system manufactured years earlier. Northern Telecom agrees with U.S. West, NYNEX, and the Toll Fraud Subcommittee recommending explicit warnings on new system equipment. However, Northern Telecom does not believe that such a requirement should be imposed retroactively. It is not possible to expect manufacturers to assume responsibility for applying warning labels to a product that left the factory many years ago.

CONCLUSION

Northern Telecom feels a strong obligation to all its customers, distributors and end users alike to help them prevent toll fraud and to help them protect their systems from unauthorized access. Northern Telecom will, as a PBX manufacturer, continue to provide the same quality of proactive support and service to combat toll fraud. Northern Telecom also pledges to work with the Commission and other sectors of the industry, in accordance with directives determined in this proceeding, to help further eliminate fraud and abuse.

Respectfully submitted,

Albert Halprin
Stephen L. Goodman
Halprin, Temple & Goodman
1100 New York Avenue, N.W.
Suite 650, East Tower
Washington, D.C. 20005
(202) 371-9100

Counsel for Northern Telecom Inc.

Of Counsel:

Thomas A. Miller
Northern Telecom Inc.
2221 Lakeside Boulevard
Richardson, Texas 75082

Dated: February 10, 1994

AMENDED IN SENATE JULY 12, 1993

AMENDED IN ASSEMBLY APRIL 14, 1993

Introduced by Assembly Member Polanco
March 4, 1993

An act to amend Section 502.7 of the Penal Code, relating to telephone fraud.

LEGISLATIVE COUNSEL'S DIGEST

AB 1656, as amended, Polanco. Fraud: telephone services.

Existing law prohibits specified activities with regard to defrauding a person providing telephone or telegraph service of the lawful charge for telephone or telegraph service. Existing law prohibits under these provisions a person from knowingly, willfully, and with intent to defraud a person providing telephone or telegraph service, avoiding or attempting to avoid, or aiding, abetting, or causing another to avoid the lawful charge, in whole or in part. for telephone or telegraph service by any of specified means, including, by using any deception, false pretense, trick, scheme, device, or means.

This bill would add to the prohibitions covered by this provision the use of conspiracy and the fraudulent use of false, altered, or stolen identification to defraud a person providing telephone or telegraph service.

Existing law makes a violation of these prohibitions a misdemeanor or a felony if the total value of all telephone or telegraph services obtained in violation of the provisions aggregates over $400 within any period of 12 consecutive months during the 3 years immediately prior to the indictment, certification to superior court, or filing of the information, or if the defendant has previously been convicted of an offense in excess of $400 under these provisions, or under similar other state or federal laws.

This bill, among other things, would revise the punishment for a violation of these provisions. This bill, instead, would provide that a theft of any telephone or telegraph services under these provisions is a misdemeanor or felony, except that theft of these services [having a] [single or aggregate value in excess of $400, or] by a person who has a prior misdemeanor or felony conviction for the theft of the services under these provisions within the past 5 years, is a felony.

Existing law also prohibits any person from publishing, as defined, the number or code of an existing, canceled, revoked, expired, or nonexistent credit card, or the numbering or coding which is employed in the issuance of credit cards, with the intent that it be used or with knowledge or reason to believe that it will be used to avoid the payment of any lawful telephone or telegraph toll charge, punishable as a misdemeanor.

This bill would include within the definition of publishing for the purpose of this provision the communication of information to any one or

DELETED MATERIAL IS IN BRACKETS []. ADDED MATERIAL IS CAPITALIZED.

more persons by electronic means, including, but not limited to, a bulletin board system, thereby imposing a state-mandated local program by expanding the scope of a crime.

This bill would also provide that any person who is the issuee of a calling card, credit card, calling code, or any other means or device for the legal use of telecommunications services and who receives anything of value for knowingly allowing another person to use the means or device in order to fraudulently obtain telecommunications services is guilty of a misdemeanor or a felony punishable pursuant to these provisions.

Because this bill would create a new crime, it would impose a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

SECTION 1. Section 502.7 of the Penal Code is amended to read:

502.7. (a) Any person who, knowingly, willfully, and with intent to defraud a person providing telephone or telegraph service, avoids or attempts to avoid, or aids, abets or causes another to avoid the lawful charge, in whole or in part, for telephone or telegraph service by any of the following means is guilty of a misdemeanor or a felony, except as provided in subdivision (g):

(1) By charging the service to an existing telephone number or credit card number without the authority of the subscriber thereto or the lawful holder thereof.

(2) By charging the service to a nonexistent telephone number or credit card number, or to a number associated with telephone service which is suspended or terminated, or to a revoked or canceled (as distinguished from expired) credit card number, notice of the suspension, termination, revocation, or cancellation of the telephone service or credit card having been given to the subscriber thereto or the holder thereof.

(3) By use of a code, prearranged scheme, or other similar stratagem or device whereby the person, in effect, sends or receives information.

(4) By rearranging, tampering with, or making connection with telephone or telegraph facilities or equipment, whether physically, electrically, acoustically, inductively, or otherwise, or by using telephone or telegraph service with knowledge or reason to believe that the rearrangement, tampering, or connection existed at the time of the use.

(5) By using any other deception, false pretense, trick, scheme, device, conspiracy, or means, including the fraudulent use of false, altered, or stolen identification.

(b) Any person who does either of the following is guilty of a misdemeanor or a felony, except as provided in subdivision (g):

(1) Makes, possesses, sells, gives, or otherwise transfers to another, or offers or advertises any instrument, apparatus, or device with intent to use it or with knowledge or reason to believe it is intended to be used to avoid any lawful telephone or telegraph toll charge or to conceal the existence or place of origin or destination of any telephone or telegraph message.

(2) Sells, gives, or otherwise transfers to another or offers, or advertises plans or instructions for making or assembling an instrument, apparatus, or device described in paragraph (1) of this subdivision with knowledge or reason to believe that they may be used to make or assemble the instrument, apparatus, or device.

(c) Any person who publishes the number or code of an existing, canceled, revoked, expired, or nonexistent credit card, or the numbering or coding which is employed in the issuance of credit cards, with the intent that it be used or with knowledge or reason to believe that it will be used to avoid the payment of any lawful telephone or telegraph toll charge is guilty of a misdemeanor. Subdivision (g) shall not apply to this subdivision. As used in this section, ``publishes'' means the communication of information to any one or more persons, either orally, in person or by telephone, radio, or television, or electronic means, including, but not limited to, a bulletin board system, or in a writing of any kind, including without limitation a letter or memorandum, circular or handbill, newspaper, or magazine article, or book.

(d) Any person who is the issuee of a calling card, credit card, calling code, or any other means or device for the legal use of telecommunications services and who receives anything of value for knowingly allowing another person to use the means or device in order to fraudulently obtain telecommunications services is guilty of a misdemeanor or a felony, except as provided in subdivision (g).

(e) Subdivision (a) applies when the telephone or telegraph communication involved either originates or terminates, or both originates and terminates, in this state, or when the charges for service would have been billable, in normal course, by a person providing telephone or telegraph service in this state, but for the fact that the charge for service was avoided, or attempted to be avoided, by one or more of the means set forth in subdivision (a).

(f) Jurisdiction of an offense under this section is in the jurisdictional territory where the telephone call or telegram involved in the offense originates or where it terminates, or the jurisdictional territory to which the bill for the service is sent or would have been sent but for the fact that the service was obtained or attempted to be obtained by one or more of the means set forth in subdivision (a).

(g) Theft of any telephone or telegraph services under this section[ ] [having a single or aggregate value in excess of four hundred dollars] [($400), or] by a person who has a prior misdemeanor or felony conviction for theft of services under this section within the past five years, is a felony.

(h) Any person or telephone company defrauded by any acts prohibited under this section shall be entitled to restitution for the entire amount of the charges avoided from any person or persons convicted under this section.

(i) Any instrument, apparatus, device, plans, instructions, or written publication described in subdivision (b) or (c) may be seized under warrant or incident to a lawful arrest, and, upon the conviction of a person for a violation of subdivision (a), (b), or (c), the instrument, apparatus, device, plans, instructions, or written publication may be destroyed as contraband by the sheriff of the county in which the person was convicted or turned over to the person providing telephone or telegraph service in the territory in which it was seized.

(j) Any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any public offense described in this section or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of this section shall be subject to forfeiture.

SEC. 2. No reimbursement is required by this act pursuant to Section 6 of Article XIIIB of the California Constitution because the only costs which may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, changes the definition of a crime or infraction, changes the penalty for a crime or infraction, or eliminates a crime or infraction. Notwithstanding Section 17580 of the Government Code, unless otherwise specified in this act, the provisions of this act shall become operative on the same date that the act takes effect pursuant to the California Constitution.

MCS Multimedia Communication Systems

Attachment B

Sales and Marketing Bulletin

Number: 888-G

Date: November 1993

Meridian 1 Software

Meridian 1 System Security Management; NTP Section

Distributors and end users have requested that Meridian 1 security information be consolidated into one NTP section providing a single reference point for Meridian 1 security features. The NTP section (553-3001-302) provides information about the security features as well as their implementation. To assist with new system configurations and existing system evaluations, Audit Guidelines and Installation sections are included in the NTP.

The *Controlling Access Privileges Workbook* (P0735064) currently shipped with all systems and upgrades will be replaced by the above NTP beginning January 3, 1994. The *Controlling Access Privileges Workbook* will continue to be available and will be updated to include new features added with Meridian 1 software and Meridian Mail releases. Orders for the *Controlling Access Privileges Workbook* can be placed through Northern Telecom Nashville at (800) 321-2649.

NTP Ordering Information

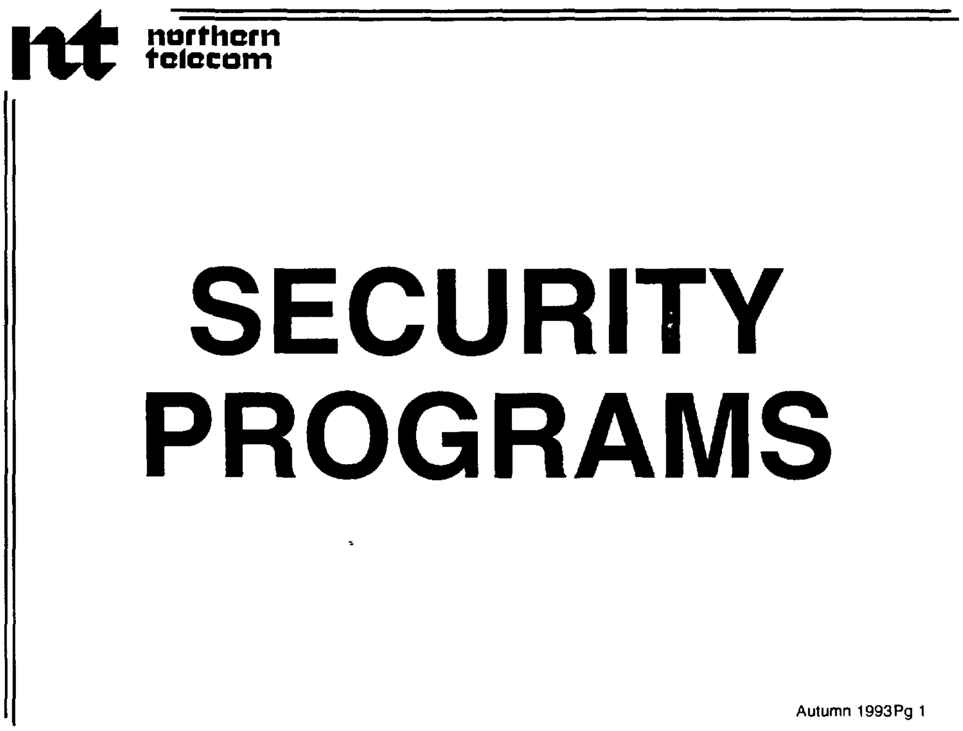
The Meridian 1 System Security Management NTP section is included in the following Northern Telecom Publications.

Order Code	Description
P0746472	Condensed X11 System Management Overview, Applications & Security
P0746460	X11 System Management Overview, Applications & Security Guide

Note: Orders for these guides will be accepted after January 3, 1994.

If a copy of the NTP is required prior to the January 3, 1994 publication date or you have any questions regarding the NTP section or any other Meridian 1 Security Program, contact Mary Lord at (214) 684-8285 or via FAX at (214) 684-3813.

Meridian 1 and SL-1 are trademarks of Northern Telecom.

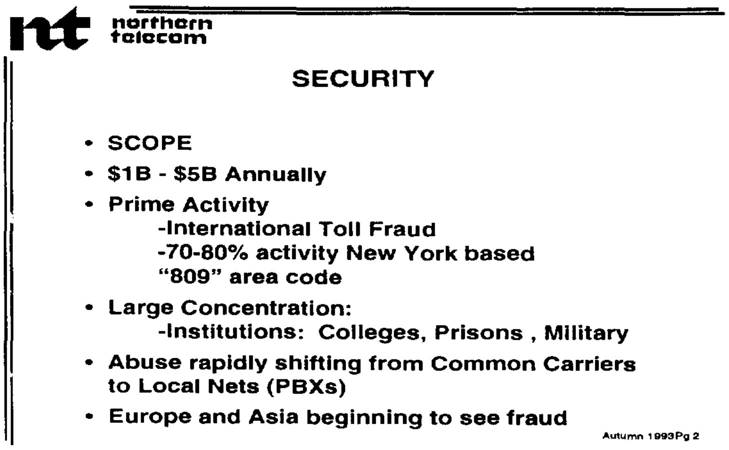


northern telecom

SECURITY PROGRAMS

Autumn 1993Pg 1

Meridian 1 Security Programs received its official status in 1992 as a result of the Controlling Access Privileges program. This program began in 1990 with the on-set of Toll Fraud as a major problem for PBX owners. Today, its major focus is still education for the distributor and the end-user.



northern telecom

SECURITY

- SCOPE
- $1B - $5B Annually
- Prime Activity
  -International Toll Fraud
  -70-80% activity New York based
  "809" area code
- Large Concentration:
  -Institutions: Colleges, Prisons , Military
- Abuse rapidly shifting from Common Carriers to Local Nets (PBXs)
- Europe and Asia beginning to see fraud

Autumn 1993Pg 2

The problem of toll fraud is estimated to be between $1B and $5B annually. Most authorities feel this estimate is low. Many victims don't report their losses and there is no central reporting structure.

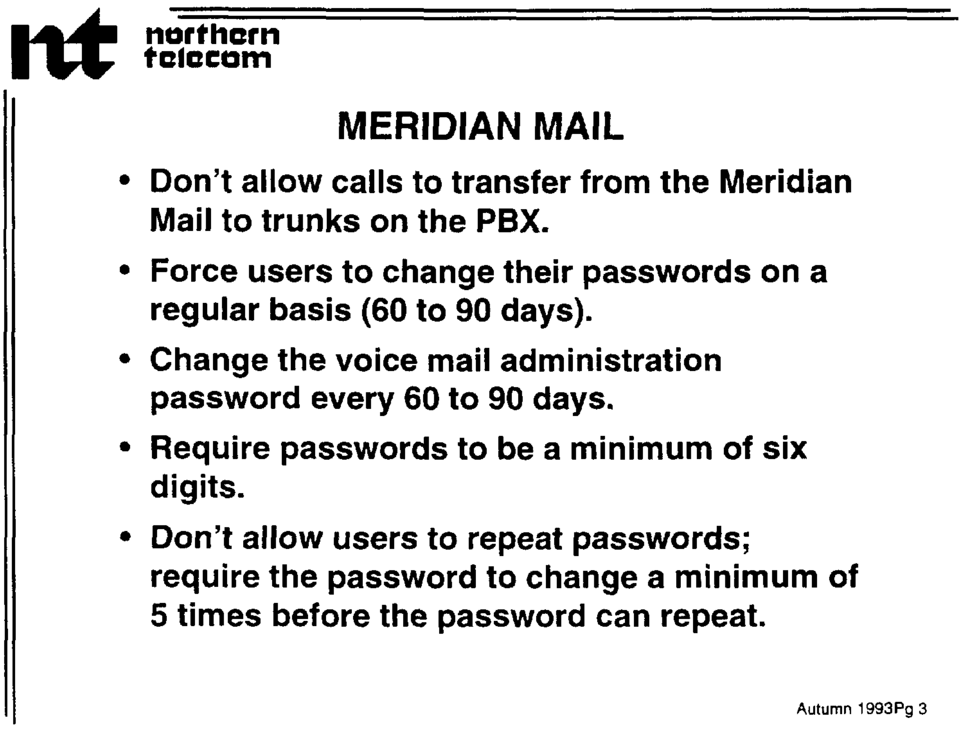
Most calls originate in the New York City area and terminate in the Dominican Republic. Call-Sell operators use stolen credit cards, DISA numbers, and unprotected voice mail systems to place unauthorized toll calls to the 809 area code. The buyers pay $10 to $30 for long distance calls from pay phones in public areas, or key systems in private homes. Long distance carrier rates would be much higher for these international calls and many times Call-Sell operators will let their customers talk as long as they wish.

Any place where there are many people far from home becomes fertile ground for call-sell operations. The dormitories on a college campus, the barracks on a military base or the common areas in a prison are all places to sell long distance calls at reduced rates.

Prisoners use social engineering scams to obtain free long distance service by posing as law enforcement officers, representatives of long distance carriers, and physicians needing assistance in emergency situations.

The common carrier has security in place to determine fraud taking place using their long distance facilities and credit cards. However inter exchange carriers will all advise you that they are your last line of defense. You are your first line defense. Phone phreaks and hackers prey on PBX owner's complacency, lack of education or unprotected access to long distance facilities.

The international market also sees fraud in ever increasing instances as hackers penetrate global companies and international 800 facilities.



northern telecom

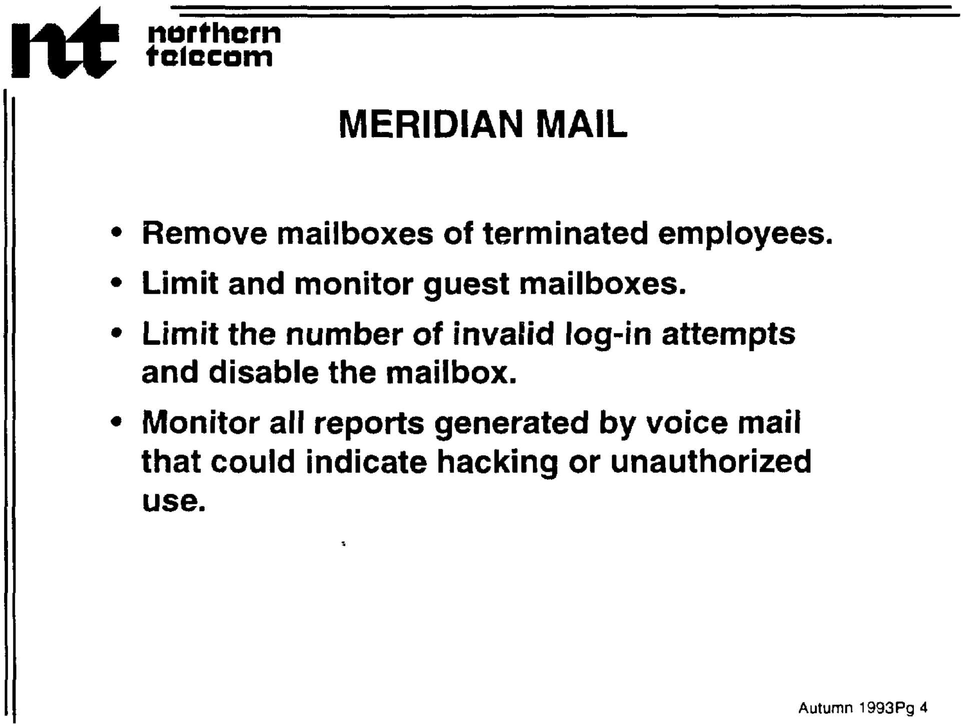
MERIDIAN MAIL

- **Don't allow calls to transfer from the Meridian Mail to trunks on the PBX.**
- **Force users to change their passwords on a regular basis (60 to 90 days).**
- **Change the voice mail administration password every 60 to 90 days.**
- **Require passwords to be a minimum of six digits.**
- **Don't allow users to repeat passwords; require the password to change a minimum of 5 times before the password can repeat.**

Autumn 1993Pg 3

Protect your Meridian Mail by blocking trunk access codes, Special Prefix codes and BARS/NARS access codes. This one common oversight is the main cause of toll fraud today. All Meridian Mail systems beginning with Release 7.54 are fully restricted at shipment. The system must be programmed to allow calls to exit the Meridian Mail and access long distance facilities. Use the "force password change" ability of the Mail to change mailbox passwords every 60 to 90 days. Make the minimum password six digits in length. Don't allow users to repeat passwords until the password has been changed a minimum of five times.

Release 8 Meridian Mail introduces the forced password change on the administration terminal. Users are forced to change the default password upon first log in. Continue this maintenance by changing the admin password every 60 to 90 days.



northern telecom

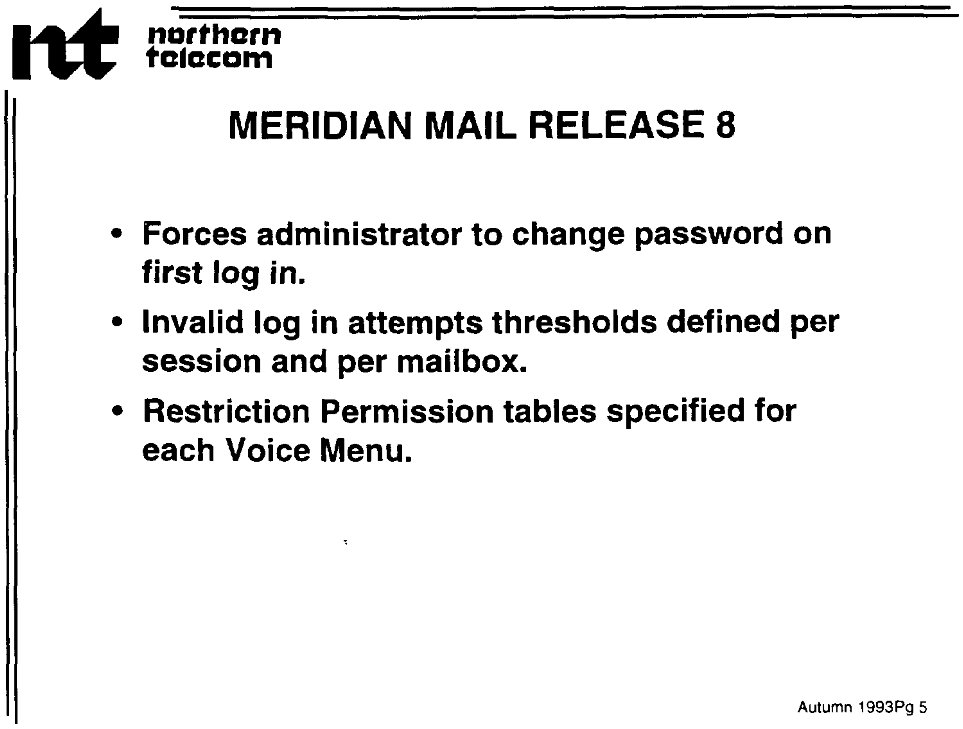
MERIDIAN MAIL

- **Remove mailboxes of terminated employees.**
- **Limit and monitor guest mailboxes.**
- **Limit the number of invalid log-in attempts and disable the mailbox.**
- **Monitor all reports generated by voice mail that could indicate hacking or unauthorized use.**

Autumn 1993Pg 4

When employe are terminated, remove their mailboxes. Vacant mailboxes are a hacker's favorite prey. If the hacker succeeds in breaking the password, he can change the personal greeting into an information line detailing stolen VISA, Mastercard, American Express, and telephone credit card numbers with all the adjunct information including expiration date and social security numbers. The hackers sell the DID numbers into the mailbox for a fee and the callers receive stolen information to user at their own discretion. They can also change the personal greeting so that it sounds like someone accepting 3rd party billing charges from an operator. The personal greeting sounds like, "Hello? (long pause) Yes operator, I'll accept the charges."

The same scam applies to guest mailboxes. Be certain to monitor and limit the number of guest mailboxes. Disable all mailboxes after three invalid log in attempts. Frustrate the hacker and make his efforts more difficult. Review voice mail reports and concentrate on areas that would indicate hacker activity such as high storage, invalid log in attempts and higher than normal access activity, especially on evenings, holidays and weekends.



northern
telecom

MERIDIAN MAIL RELEASE 8

- **Forces administrator to change password on first log in.**
- **Invalid log in attempts thresholds defined per session and per mailbox.**
- **Restriction Permission tables specified for each Voice Menu.**

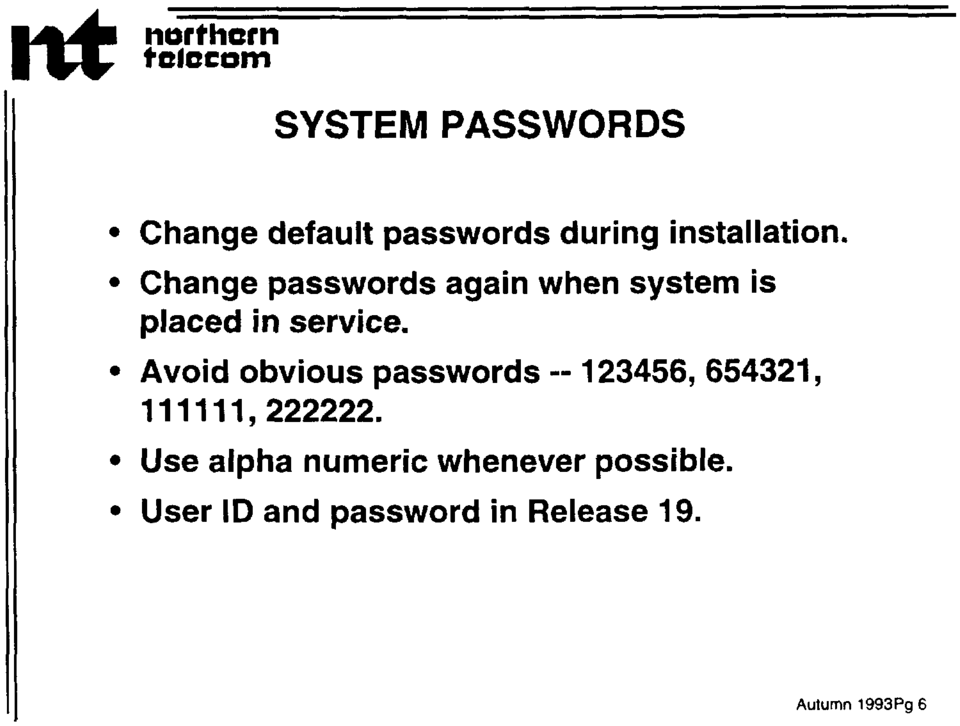
Autumn 1993Pg 5

The administrator is forced to change the default password on first log in for Meridian Mail Release 8. This measure reduces the ability of the hacker to disable security restrictions and to create new mailboxes for code lines or 3rd party billing scams. Northern Telecom recommends the administrator password be changed every 60 to 90 days.

In besides defining the number of invalid log-in attempts per mailbox, the administrator can also define the number of invalid log-in attempts per session. The hacker who locks up one mailbox after another while searching for easy access will find this feature can limit his activities to only one mailbox at a time.

Restriction Permission tables for external call enter and AMIS networks are also available.

The Restriction Permission tables can now be specified for each Voice Menu instead of applying one table for all menus. Additionally, each menu may have an optional table, configured specifically to the menu as opposed to one of the four standard tables.



northern telecom

SYSTEM PASSWORDS

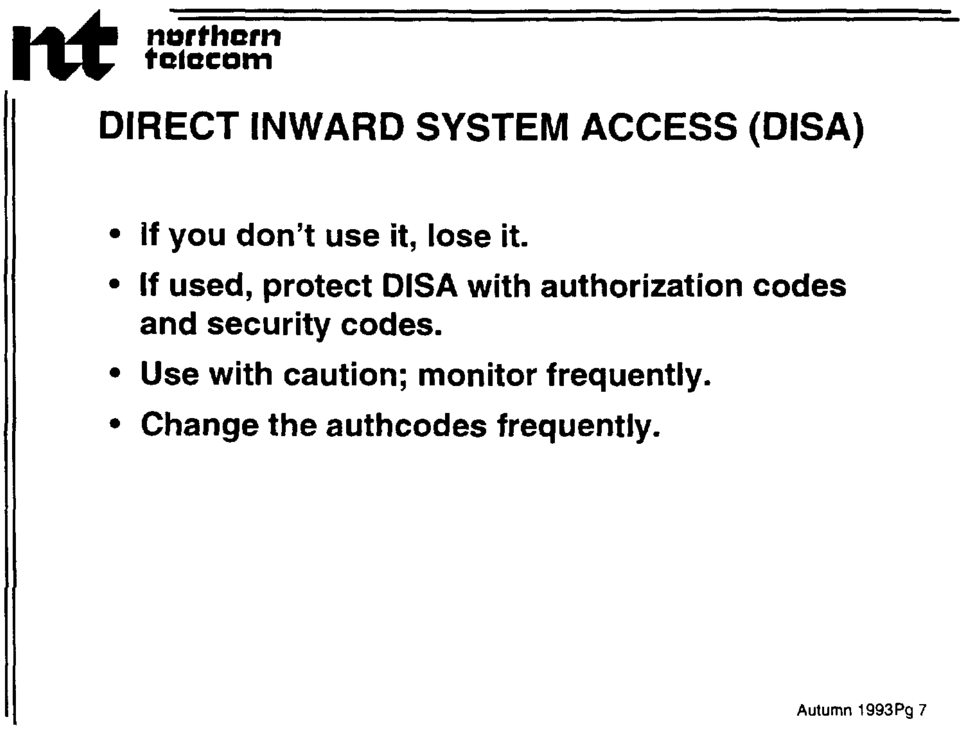
- **Change default passwords during installation.**
- **Change passwords again when system is placed in service.**
- **Avoid obvious passwords -- 123456, 654321, 111111, 222222.**
- **Use alpha numeric whenever possible.**
- **User ID and password in Release 19.**

Autumn 1993Pg 6

The passwords to your system are much like the keys to your car. A car with the door unlocked, the keys in the ignition and the engine running is an invitation most car-jackers would find hard to resist. Hackers love default passwords in much the same way; and users who don't change the default passwords during installation will find hackers on their doorstep sooner than they could ever imagine. Northern Telecom recommends changing the default passwords during installation and again after systems have been placed in service. Almost 40% of new systems are hacked or attempted within six weeks after installation.

Avoid obvious passwords. Hackers only try 11% of all possible number combinations. They usually are successful because users prefer numbers that are easy to remember. Alpha numeric passwords are the most difficult to break. Try using two words concatenated with a number such as HOT5DOG or COOL778BEANS.

Use Limited Access to Overlays to restrict system access and create an Audit Trail to know who logged on when and what overlays were accessed.



northern telecom

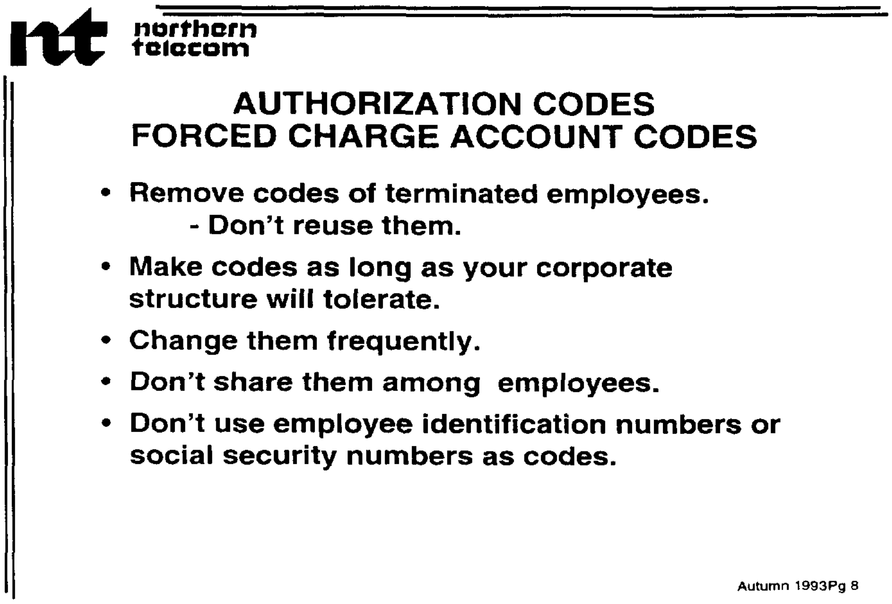
DIRECT INWARD SYSTEM ACCESS (DISA)

- If you don't use it, lose it.
- If used, protect DISA with authorization codes and security codes.
- Use with caution; monitor frequently.
- Change the authcodes frequently.

Autumn 1993Pg 7

Northern Telecom no longer ships Direct Inward System Access (DISA) as a standard feature of the base software package. Customers may still order the feature with new systems at no charge, using a separate order number. Northern Telecom recommends customers using DISA protect the option with the use of security codes and authorization codes. Monitor the feature frequently and change the authorization codes on a regular basis.

Option 11 customers can order software without DISA beginning in Release 18 (1994).



northern telecom

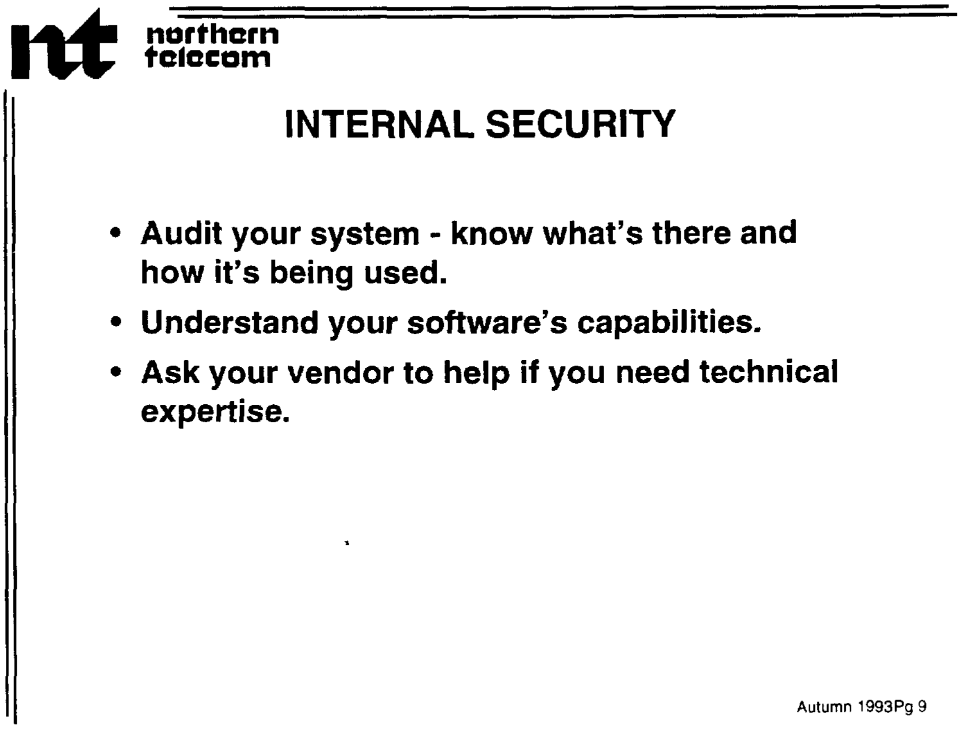
AUTHORIZATION CODES
FORCED CHARGE ACCOUNT CODES

- Remove codes of terminated employees.
    - Don't reuse them.
- Make codes as long as your corporate structure will tolerate.
- Change them frequently.
- Don't share them among employees.
- Don't use employee identification numbers or social security numbers as codes.

Autumn 1993Pg 8

Authorization codes are an important security protection for systems using DISA and restricted phones. The maintenance of authorization codes often requires a link to your human resources or personnel department. Have them notify you when employees leave the company so that you can remove the authcodes of terminated employees. Don't reuse the codes. Authcodes should be at least eight digits in length. In this case, more is better; the longer the authcode, the more difficult it is for the hacker to break. Change the codes frequently. Don't share the codes within departments; give each employee their own code and make them responsible for them by providing CDR printouts of their calls. Don't use common denominators for the code source. Employee home phone numbers, social security numbers, identification numbers or department numbers are poor choices. This type of information can be gleaned from a dumpster and hackers have all night long for demon dialers to find a good authorization code.

Maintenance of authorization codes often requires a link to your human resources or personnel department. Have them notify you when employees leave the company so that you can remove the authcodes of terminated employees. Don't reuse the codes. Authcodes should be at least eight digits in length. In this case, more is better; the longer the authcode, the more difficult it is for the hacker to break. Change the codes frequently. Don't share the codes within departments; give each employee their own code and make them responsible for them by providing CDR printouts of their calls. Don't use common denominators for the code source. Employee home phone numbers, social security numbers, identification numbers or department numbers are poor choices. This type of information can be gleaned from a dumpster and hackers have all night long for demon dialers to find a good authorization code.



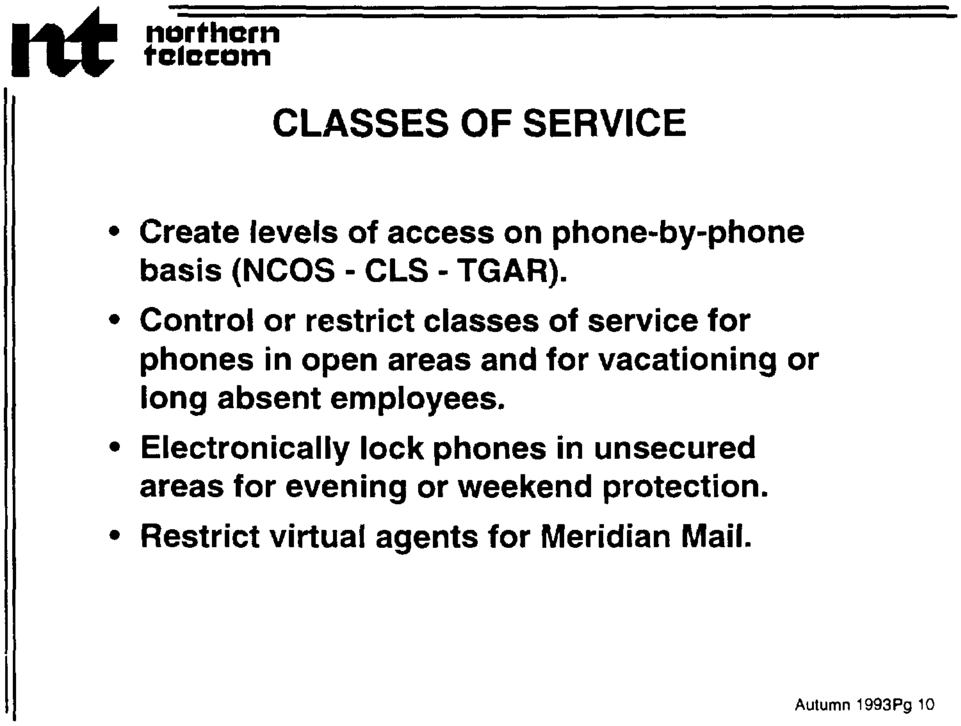
northern telecom

INTERNAL SECURITY

- Audit your system - know what's there and how it's being used.
- Understand your software's capabilities.
- Ask your vendor to help if you need technical expertise.

Autumn 1993Pg 9

The place to start the security evaluation of your system is at the PBX level. Audit your system software, evaluate its capabilities and eliminate or limit features based on usage, security or need. Northern Telecom distributors are able to help you evaluate your system and its capabilities.



northern telecom

CLASSES OF SERVICE

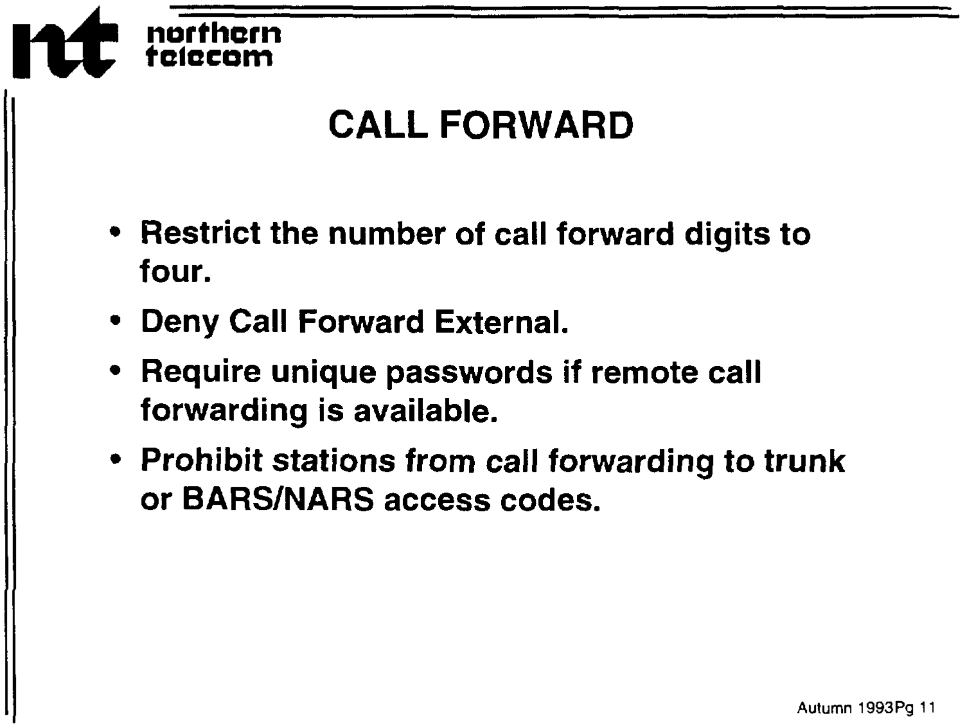
- **Create levels of access on phone-by-phone basis (NCOS - CLS - TGAR).**
- **Control or restrict classes of service for phones in open areas and for vacationing or long absent employees.**
- **Electronically lock phones in unsecured areas for evening or weekend protection.**
- **Restrict virtual agents for Meridian Mail.**

Autumn 1993Pg 10

The eight levels for class of service combine with the 99 levels of Network Class of Service and the 31 levels of Trunk Group Access Restriction to form levels of access on a phone by phone basis. These controls can limit calling area and direct access as well as inward access in some cases.

Be sure to invoke controls such as controlled class of service to lower the class of service for employees on leave or phones in open areas such as reception or conference room phones. The class of service can be raised to accommodate callers when necessary. Allow electronic lock functions for phones in cubicles or unlocked work environments; this permits the user to lock the phone when leaving, protecting the phone from unauthorized use.

Hackers often exit voice mail systems by entering digit strings that confuse the voice mail system. In an attempt to release the call, the voice mail system will transfer the call back to the PBX for processing. At this point the virtual agent linking the PBX to the voice mail is in control. If the agent is unrestricted, so is the hacker. Restrict voice mail ports to internal or local only capabilities. Remember, even though there is no phone attached to the port, there are still software features that can be activated from the port.

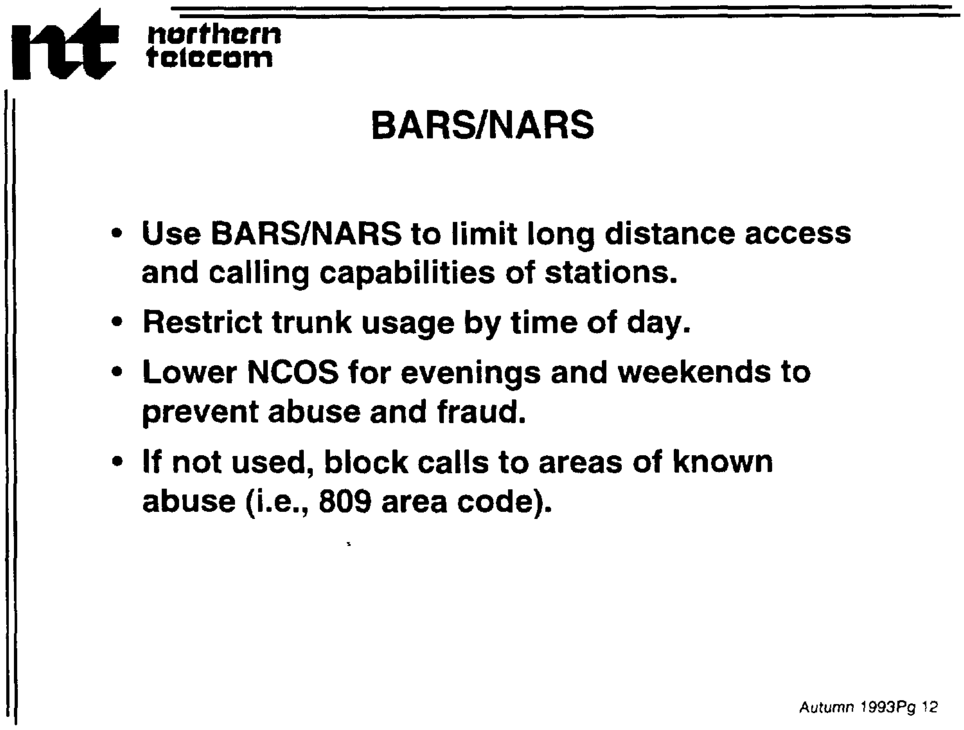


northern telecom

CALL FORWARD

- **Restrict the number of call forward digits to four.**
- **Deny Call Forward External.**
- **Require unique passwords if remote call forwarding is available.**
- **Prohibit stations from call forwarding to trunk or BARS/NARS access codes.**

Call forwarding phones to access codes is a common form of abuse. Calls to the DID number return dial tone, allowing the caller to place long distance calls. Be sure to limit the number of call forward digits to the least amount required. Four is recommended, unless the dialing plan precludes that option. Restrict external call forward on a phone by phone basis and don't allow users to call forward to trunk access codes or BARS/NARS access codes. If remote call forward is a frequently used feature, make sure each phone has its own unique password to activate this feature.



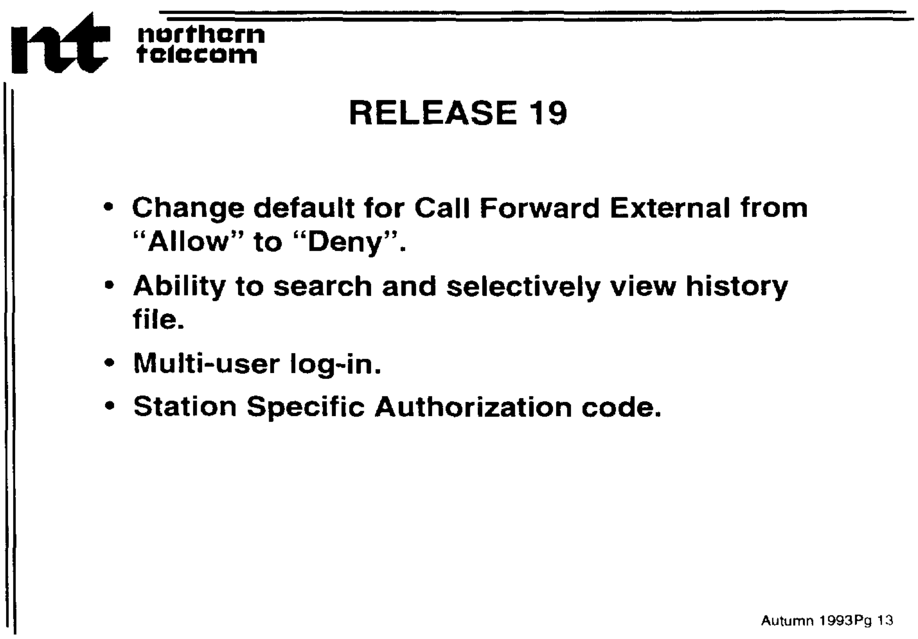
northern telecom

BARS/NARS

- **Use BARS/NARS to limit long distance access and calling capabilities of stations.**
- **Restrict trunk usage by time of day.**
- **Lower NCOS for evenings and weekends to prevent abuse and fraud.**
- **If not used, block calls to areas of known abuse (i.e., 809 area code).**

Autumn 1993Pg 12

The capabilities of Basic and Network Automatic Route selection enable the administrator to limit the calling areas of users on a phone by phone basis. Not all users need access to everywhere. Use BARS/NARS to limit users to local calls, intrastate, regional or area code only if access to international or interstate calls is not required. Time of Day Schedules limit the access of Route List Indexes to specific times during the day, restricting expensive routes to overflow abilities at certain times. TOD schedules can also restrict access to larger trunk routes after specified times. Lowering the NCOS of phones and DISA callers for evening and weekends, limits calling in off hours and reduces toll abuse from internal sources. Callers who need long distance calling capabilities in restricted hours can override the NCOS with authorization codes. Forcing callers to use BARS/NARS also enables the ability to block calls to specific area codes such as 809, or to international destinations.



northern telecom

RELEASE 19

- Change default for Call Forward External from "Allow" to "Deny".
- Ability to search and selectively view history file.
- Multi-user log-in.
- Station Specific Authorization code.

Autumn 1993Pg 13

Release 19 adds many new features and enhancements to X11 software that provide additional security features. All the features will be discussed in detail in the X11 Release 19 portion of the presentation, but the items affecting security are summarized here.

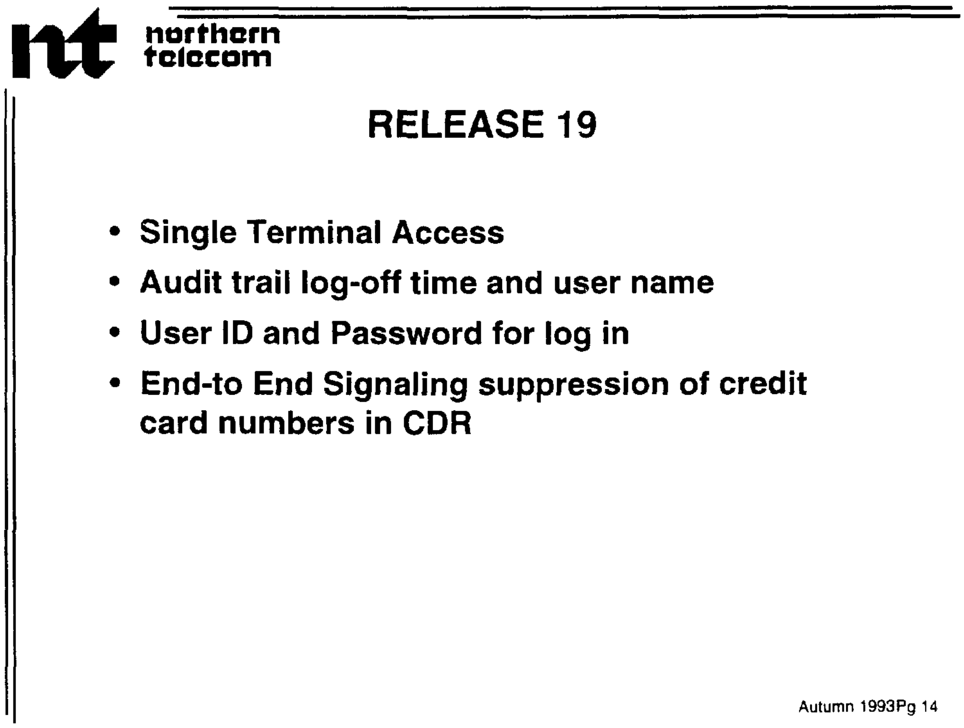
The default for Call Forward External changes from Allow to Deny. This prohibits users from call forwarding to trunk or BARS/NARS access codes.

The Automatic Set Relocation feature has added a default password of four zeroes that reduces the accidental relocation of a phone by a user.

You can selective search or view the history file as opposed to viewing all the file or what ever has transpired since the last reading of the history file. Two additional files have been added: the traffic log and the user log. These files keep track of events in a separate file from the History File.

Multi-User log in allows more than one user to access specific overlays and permits data to be entered for the same overlay simultaneously. The caution here is that hackers can be in your system simultaneously. System messages will provide you with information regarding other users. Be aware of remote access to your system when you have accessed the system and are modifying or adding data.

The ability to assign up to six authorization codes to a specific phone limits access in open or dormitory type environments. Station Specific Authorization code was developed with this function in mind.



northern
telecom

RELEASE 19

- **Single Terminal Access**
- **Audit trail log-off time and user name**
- **User ID and Password for log in**
- **End-to End Signaling suppression of credit card numbers in CDR**

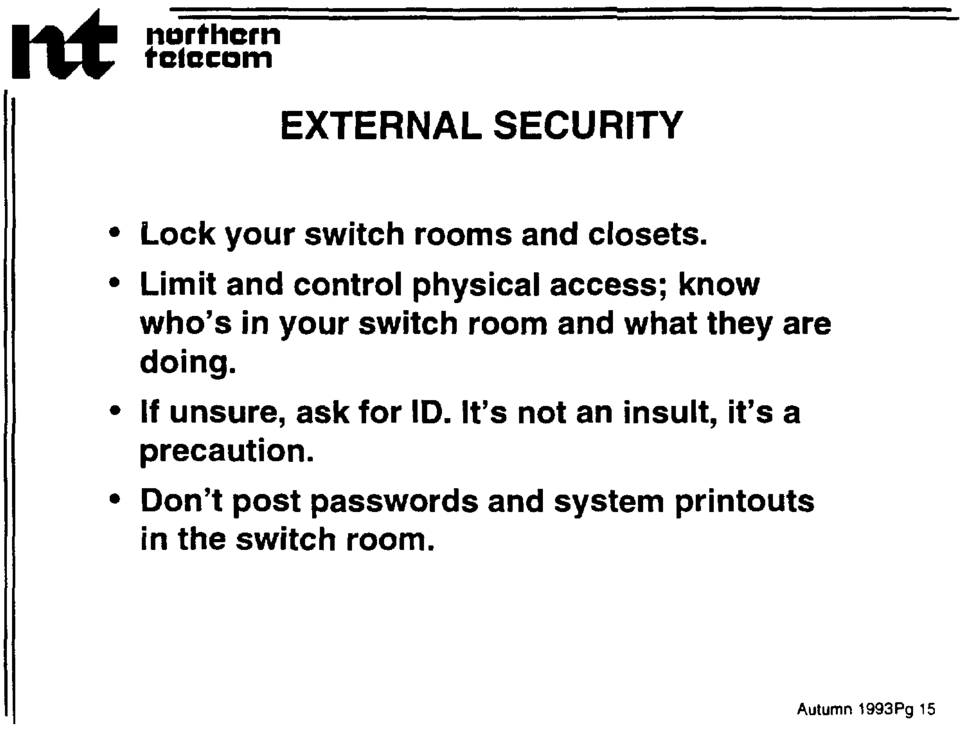
Autumn 1993Pg 14

The development of single terminal access permits the user to access more than just the Meridian 1. The terminal access now includes peripheral equipment such as voice mail, ACD MAX, and Meridian Link. It becomes even more imperative to protect this access with alpha numeric passwords of substantial length and to monitor them frequently.

The introduction of User ID and Password provide further security by requiring a match on two pieces of information. This makes random access more complicated for the hacker and provides another level of protection for you.

The audit trail available with Limited Access to Overlays has a new entry for log-off time and user name that keeps track of who was in the system when, what they accessed and how long they were there.

Using End-to End Signaling, Release 19 also permits digit suppression to keep calling card numbers from appearing on CDR records.



northern telecom

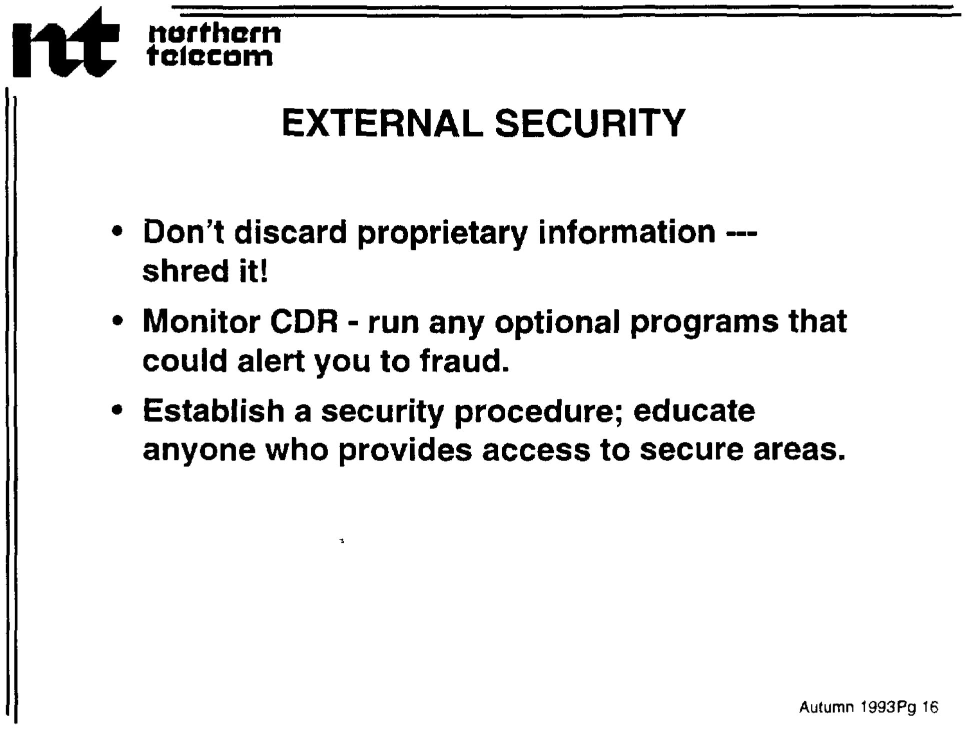
EXTERNAL SECURITY

- Lock your switch rooms and closets.
- Limit and control physical access; know who's in your switch room and what they are doing.
- If unsure, ask for ID. It's not an insult, it's a precaution.
- Don't post passwords and system printouts in the switch room.

Autumn 1993Pg 15

Customers often overlook the important element of internal security. Hackers disguised as phone company or distributor employees gain access to your switch room simply by wearing a test-set on a tool belt. More that once a user has lost valuable PBX equipment in just this fashion. Additionally, fraud takes place in equipment closets and switch rooms by simply clipping on to trunks or stations with long distance access.

Find out what other equipment is located in your switch room; who needs access and why? Know who's in your switch room. Remove system printouts from walls or cabinets. Don't display system passwords on the teletype or in plain view. Don't label he remote access modem with the public telephone number. Secure all documents. Ensure who ever enters your switch room have approved access and ask for identification if you're unsure. It's your right as a customer to know who is on your property and why.



northern telecom

EXTERNAL SECURITY

- Don't discard proprietary information --- shred it!
- Monitor CDR - run any optional programs that could alert you to fraud.
- Establish a security procedure; educate anyone who provides access to secure areas.

Autumn 1993Pg 16

Proprietary information such as CDR reports, outdated system documentation, and voice mail reports can all provide sources of information of the dumpster diver. Shred this type of information. Recyclers and disposal service providers should also be bonded. Consider it as a requisite for future contracts. Review traffic, CDR, or voice mail reports on a regular basis to determine patterns and spot unusual activity.